030238

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

MINTIC

TRD: 221.101

Bogotá D.C.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
FECHA: 13/9/2016 HORA: 10:57:05 FOLIOS: 5
REGISTRO NO: **959038**
DESTINO: FUNDACION KARISMA
BOGOTÁ-BOGOTA

Doctora
CAROLINA BOTERO CABRERA
Directora
Fundación KARISMA
Calle 59 N° 18 – 20 Of. 201
Bogotá, D.C.

Asunto: Radicado N° 763433 Análisis ciudadano sobre seguridad digital sitio web imeicolombia.com.co.

Respetada doctora Carolina,

El Ministerio de TIC aprecia enormemente la labor que viene desempeñando la Fundación KARISMA en pro del derecho ciudadano a la protección de la privacidad en línea y su comprensión y promoción en relación con la importancia de la seguridad digital.

En cuanto al documento **"Plataformas inseguras, el caso de imeicolombia.com.co"** preparado por su equipo de trabajo y en el cual describe una serie de problemas del sitio web o su "vulnerabilidad concreta", es necesario contextualizar el análisis hecho dentro de la realidad jurídica y técnica de la plataforma.

Las consideraciones del análisis de la Fundación se circunscriben al sitio web de consulta http: //www.imeicolombia.com.co/ConsultaPublicaIMEI/, (en adelante IMEI COLOMBIA), portal a través del cual se consulta de manera pública un IMEI (identificador único que tiene cada teléfono móvil) para determinar si está reportado en la base de datos negativa y la causal por la cual se reportó, es decir, si fue por hurto, extravío o no registro.

Sea lo primero aclarar que la página IMEI COLOMBIA, si bien forma parte de la estrategia del gobierno nacional contra el hurto celular, no es una página a cargo de Min TIC u otra entidad del Estado, sino que es administrada por la empresa ***Informática el Corte Inglés S.A.***, en su calidad de Administrador de las Bases de Datos - ABD, quien ha sido contratada por los proveedores de redes y servicios de telecomunicaciones móviles-PRSTM, para el cumplimiento de obligaciones derivadas de lo dispuesto en el artículo 106 de la Ley 1453 de 2011. Según el mencionado artículo, las bases de datos tanto positivas como negativas, que contengan la información de identificación de equipos terminales móviles, deberán ser implementadas y administradas de manera centralizada, a través de un tercero, por parte de los PRSTM y la información consignada en dichas bases de datos tendrá carácter público, sin perjuicio de la información que contenga datos personales, la cual será protegida de conformidad con lo establecido por la ley.

En desarrollo de la norma citada, la CRC estableció dentro de las obligaciones del Administrador de las Bases de Datos[1] la de "*4.14 Suministrar las herramientas e interfaces adecuadas para la realización de consultas en línea, registro a registro, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, la CRC y demás organismos autorizados para acceder a la BDA. Así mismo, poner a disposición del público una consulta vía Web registro a registro, de los IMEIs que se encuentren incluidos en la base de datos negativa*". (SFT)

De acuerdo con el marco legal y reglamentario, la consulta pública de los IMEI y la razón de su inclusión en la base de datos negativa, tiene sustento legal como una obligación de los PRST, la cual deben ejecutar a través de un tercero. Es de indicar, que la información que se entrega al público no contiene datos personales objeto de protección, a la luz de la Ley 1581 de 2012, guardando congruencia con lo conceptuado por la Superintendencia de Industria y Comercio como autoridad del país en la materia[2] y siguiendo las mejores prácticas de terceros países que revisten de una alta protección a tal tipo de datos[3].

---

[1] artículo 4 de la resolución CRC 3128 de 2011

[2] Concepto del 2016-01-22 con Radicado No. 16-1266- -2-0. (en donde se explicó lo siguiente: "*Descendiendo al cuestionamiento bajo análisis, el dato personal corresponde a toda pieza de información relativa a una persona natural que puede ser determinada o determinable mediante distintos identificadores, por ejemplo, el IMSI y el IMEI, toda vez que* ***si bien dichos códigos pueden no estar relacionados con una persona determinada,*** *a partir de su asociación con datos adicionales se puede llegar a individualizar al titular*")

[3] Personal Data Protection Commission, Singapore, Proposed Advisory Guidelines on the Application of the Personal Data Protection Act to Scenarios faced in the Telecommunication Sector, p. 8 (en donde se dispuso lo siguiente: "*Various numbers are used in connection with the operation of a telecommunication network, for example, to identify particular equipment that is connected to the network. In general, such numbers are not used to directly identify an individual and hence would not, on*

Hechas las anteriores precisiones se procederá a analizar los diferentes aspectos planteados en el informe remitido por la Fundación KARISMA.

A. Sobre los Aspectos Técnicos relativos a la Seguridad Digital

1. Seguridad de la página IMEI COLOMBIA

En cuanto a la seguridad de la página IMEI COLOMBIA se debe tener en cuenta lo siguiente:

- La consulta del IMEI se realiza a una Base de Datos Negativa imagen (repositorio en copia) de la Base de Datos Negativa principal. En ningún momento se ofrece acceso desde la consulta en el portal IMEI Colombia a la base de datos negativa principal, ni a ninguna otra fuente de información.

- La información que está devolviendo el enlace web de IMEI Colombia corresponde al IMEI que ingresó el usuario y a la causal por la cual fue incluido en la Base de Datos Negativa, en caso que éste se encuentre allí reportado.

- En cuanto a la sugerencia de cifrado del IMEI, debe tenerse claro que el IMEI no es un dato que se extraiga de la BD negativa, sino que por el contrario es digitado por el usuario a efectos de la consulta y de poder determinar si el equipo tiene algún reporte por hurto, extravío o bloqueo por no registro. En este mismo sentido, no se realiza ninguna operación de registro / almacenamiento en la BD negativa, sólo consulta y el resultado de la misma.

2. Sobre la vulnerabilidad del servidor web [redacted]

El servidor web que sirve la página es parte del Servidor de aplicaciones [redacted] que, tal y como se indica en el informe mencionado, sirve las páginas de la consulta pública de IMEI de la República de Colombia (http://www.imeicolombia.com.co).

their own, be considered personal data. One such example is the IMEI number (...) As with any other network identifier such as an Internet Protocol ("IP") address, an IMEI number may not be personal data when viewed in isolation, because it simply identifies a networked device.")

Ahora bien, es importante resaltar que la vulnerabilidad [redacted] no aplica [redacted]

[redacted]

Si además se analizan las vulnerabilidades [redacted] se observa que no sufre la vulnerabilidad mencionada en dicho informe:

De otra parte, el informe en comento hace referencia a la siguiente vulnerabilidad,

Al respecto, cabe precisar que la misma hace referencia a [redacted] y a la [redacted], componentes usados para programar con [redacted] y no usados [redacted]. Finalmente, la versión [redacted] y siguientes que se mencionan en el informe y en la explicación de la vulnerabilidad son versiones de las librerías [redacted] que se no se usan [redacted].

3. Encriptación de los datos/HTTPS

Actualmente, las páginas de las que dispone el portal IMEI Colombia se presentan sin cifrar, ya que no usan el protocolo SSL para su cifrado.

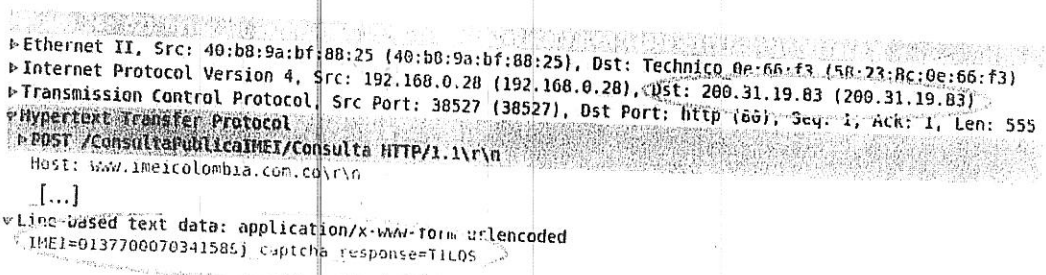
No obstante lo anterior, es importante mencionar que la consulta de IMEI es la única página pública del sitio, y ésta no presenta, ni registra ningún dato que esté clasificado como sensible o que pueda ser usado con propósito de acceder a datos que exijan medidas de control particular, conforme lo señalado en la ley[4].

La consulta verifica si un IMEI está en la Base de Datos Negativa y, en respuesta a dicha consulta, se arroja como resultado si dicho identificador está o no en la mencionada BDA Negativa. En el evento en que dicho IMEI esté incluido en la misma, se obtiene información sobre los PRSTM que lo incluyeron y el motivo de su inclusión (hurto, extravío, bloqueo por no registro). Esto se ilustra tanto en la traza adjunta en el informe que se muestra a continuación, como en las pantallas de respuesta, así:

Traza del informe.

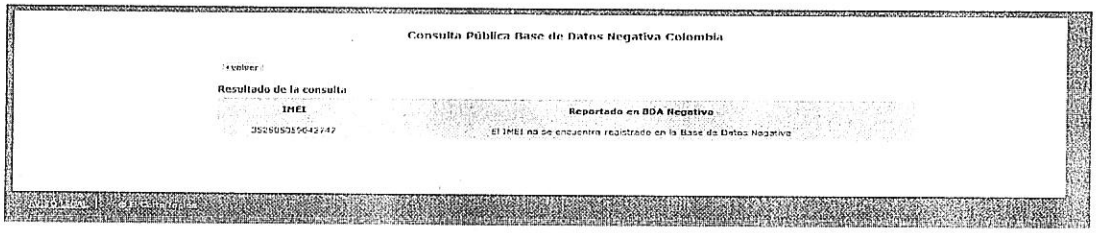
[3] Servidor destinatario del envío del número IMEI

Una búsqueda del IMEI consultado en el formulario (013770007034158), en la captura de flujo que hicimos con el programa WireShark, nos lleva a este extracto de *query* que resalta el envío del IMEI y del *captcha* hacia la dirección IP: 200.13.19.83:

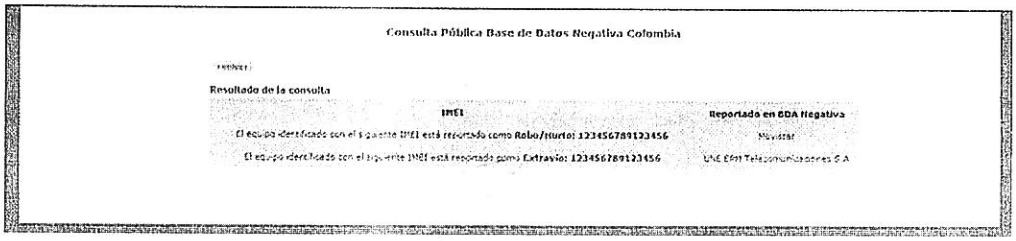


[4] Ley 1581 de 2012, **Artículo 5°. *Datos sensibles.*** Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Respuesta indicando que el IMEI no está en la BDA Negativa.



Respuesta indicando que un IMEI está en la BDA negativa con su(s) correspondiente(s) reporte(s) en el (los) Prestador(es) que pidieron la inclusión y el motivo de la misma:



Como se puede observar en las tres imágenes anteriores, no existe ningún dato sensible como objeto de transferencia o de respuesta a las consultas.

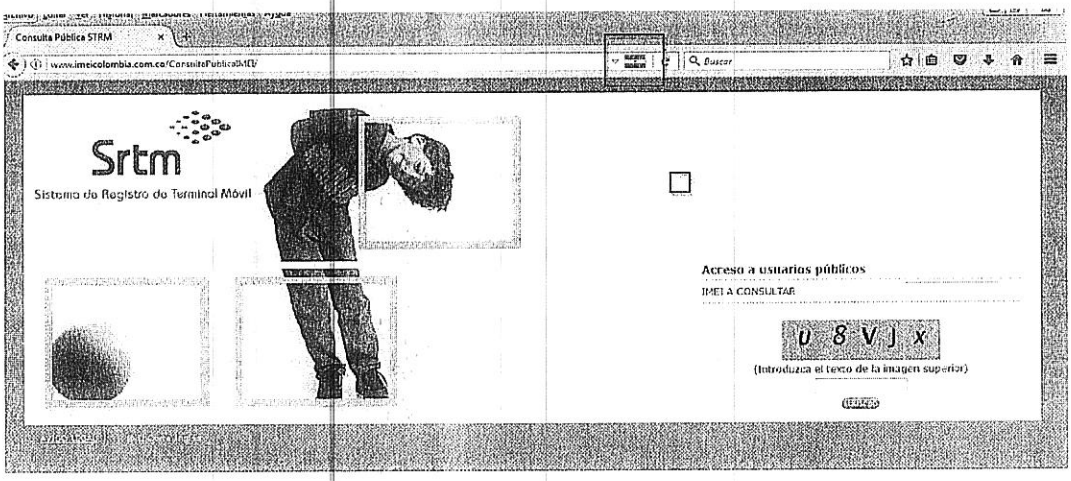
4. Respecto de la inquietud sobre ¿Dónde están mis datos?

En lo referente a la inquietud planteada, se menciona en el informe que con Flagfox se observa que el servidor web está en Argentina e incluso se sugiere la posibilidad de que la Base de Datos puede estar en Argentina.

Ahora bien, al usar Flagfox aparece la bandera de Argentina en la URL, en este caso porque la dirección pública de los sistemas, la 200.31.19.83 está asignada a Argentina ya que el proveedor de los recursos tiene una parte de las comunicaciones centralizadas en ese país, pero tal como ha sido manifestado a la CRC por *Informática El Corte Inglés*, los sistemas y las bases de datos están alojadas en Colombia en las instalaciones de la empresa por ellos escogida para tal fin.

Es importante también resaltar que la dirección IP 200.31.19.83 es la dirección pública de Internet del servicio en general, y que los servidores tienen unas

direcciones de redes internas diferentes y, que como es normal, estas no son publicadas en Internet, ni accesibles de manera pública.



5. La hora del servidor

No hay ninguna referencia a la hora en la página IMEI COLOMBIA. No obstante, los servidores del Registro de IMEI están en Colombia, incluida la Base de Datos, con el horario colombiano y se sincronizan mediante el protocolo *nttp*, siendo esto fundamental para mantener una correcta auditoria de las transacciones.

B. Sobre Las Recomendaciones sugeridas por la Fundación Karisma

A continuación se da respuesta a cada una de las recomendaciones de la Fundación:

Recomendación 1: Cambiar la presentación gráfica del sitio de modo que se identifique que es un sitio oficial del Estado si es el caso, o que ofrezca claridad sobre el hecho de que como mínimo es un sitio gestionado por privados en el marco de una campaña de gobierno y en desarrollo de una obligación legal.

Respuesta: *Se acoge la sugerencia y la misma será transmitida por MinTIC a los responsables del sitio.*

Recomendación 2: Ser transparente sobre el tipo de gestión de datos que se hace y describir la forma como se protegen. Para esto, es necesario desplegar más información en el sitio en particular redactar y publicar los textos correspondientes a la parte de "Aviso Legal". Como mínimo, se debe explicar quién es la entidad responsable del tratamiento, quien gestiona el sitio y quién almacena los datos, con indicación de los países correspondientes. De otra parte, deben desarrollarse las obligaciones legales de la Ley de Protección de Datos colombiana. Esto obligará, al menos a evaluar si están cumpliendo con la misma.

Respuesta: *En consideración a que los datos que se están tratando, aisladamente considerados, no son de carácter personal y mucho menos sensibles, los responsables del tratamiento no estarían obligados a utilizar dicho aviso legal con la formalidad sugerida. No obstante, de acuerdo con la recomendación 1, se sugerirá al administrador de la base de datos dar información más clara al usuario de la página.*

Recomendación 3: Si hay contratos de tercerización de nivel 1 y 2, es necesario asegurarse que cada uno contengan las cláusulas de confidencialidad necesarias.

Respuesta: *Son temas contemplados en los acuerdos suscritos entre los PRSTM y el ABD. En tal sentido, se revisará su alcance a fin de determinar la pertinencia de lo sugerido.*

Recomendación 4: Reemplazar el protocolo HTTP, que no es seguro, por el protocolo HTTPS que permitirá una autenticación del sitio web y la confidencialidad de los datos transmitidos.

Respuesta: *En atención a lo explicado previamente, esta es una oportunidad de mejora para el sitio web, para lo cual MinTIC realizará las gestiones ante el ABD para fortalecer su operación.*

Recomendación 5: Modificar el dominio para que la extensión no sea.com, que hace referencia a un sistema comercial.

Respuesta: *Como se indicó previamente, no es un dominio gestionado por una entidad del Estado por lo cual se analizará la posibilidad de manejar un dominio diferente.*

Recomendación 6: **Configurar el servidor web a la hora correcta (*ntpdate*).**

Respuesta: *De conformidad con lo informado por el ABD, actualmente se está utilizando el protocolo para la sincronización automática de la hora del servidor.*

Así las cosas, el Ministerio procederá de conformidad.

Cordialmente,

NICOLÁS MAURICIO SILVA CORTÉS
Director para la Industria de Comunicaciones

Proyectado por: Gloria Amparo Rico, Asesora Dirección Industria de Comunicaciones Min TIC

Revisado por:
Gina Albarracin Barrera — Directora de Vigilancia y Control Min TIC
Jorge Fernando Bejarano Lobo — Director de Estándares y Arquitectura de TI Min TIC
Christian Thowinsson Peñaranda — Jefe Oficina TI Min TIC
Sandra Milena Urrutia Pérez — Asesora Dirección Vigilancia y Control Min TIC
Claudia Ximena Bustamante O — Coord. Relaciones de Gobierno y Asesoría CRC